Guia de Elaboração de Programa de Governança em Privacidade

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Versão 1.0

Brasília, Outubro de 2020

GUIA DE ELABORAÇÃO DE PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

Lei Geral de Proteção de Dados Pessoais

MINISTÉRIO DA ECONOMIA

Paulo Roberto Nunes Guedes

Ministro

SECRETARIA ESPECIAL DE DESBUROCRATIZAÇÃO, GESTÃO E GOVERNO DIGITAL

Caio Mario Paes de Andrade

Secretário Especial de Desburocratização, Gestão e Governo Digital

SECRETARIA DE GOVERNO DIGITAL

Luis Felipe Salin Monteiro

Secretário de Governo Digital

DEPARTAMENTO DE GOVERNANÇA DE DADOS E INFORMAÇÕES

Fabiana de Assunção Cruvinel

Diretora do Departamento de Governança de Dados e Informações

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Mauro Cesar Sobrinho

Coordenador-Geral de Segurança da Informação

Equipe Técnica de Elaboração

Denis Marcelo Oliveira

Julierme Rodrigues da Silva

Loriza Andrade Vaz de Melo

Luiz Henrique do Espírito Santo Andrade

Tássio Correia da Silva

Wellington Francisco Pinheiro de Araújo

Histórico de Versões

Data	Versão	Descrição	Autor
05/10/2020	1.0	Primeira versão do Guia de Programa de Governança em Privacidade.	Equipe Técnica de Elaboração

SUMÁRIO

INTRODUÇÃO

Na administração pública, o gerenciamento da privacidade deve incluir as estratégias, habilidades, pessoas, processos e ferramentas que os órgãos e entidades precisam prover para conquistar a confiança dos servidores e dos cidadãos e, ao mesmo tempo, cumprir com exigências apresentadas nos normativos de privacidade. Um **Programa de Governança em Privacidade (PGP)** captura e consolida os requisitos de privacidade com o intuito de ditar e influenciar como os dados pessoais são manuseados no seu ciclo de vida como um todo.

Nesse sentido, este Guia orienta a elaboração de um Programa de Governança em Privacidade por órgãos e entidades da Administração Pública Federal (APF) direta, autárquica e fundacional.

E, nesse cenário, gerenciamento de segurança e risco, bem como seus respectivos responsáveis, encontram, cada vez mais, requisitos complexos e restritivos a serem cumpridos para se ter, assim, uma efetiva governança de privacidade e manuseio de dados pessoais ao longo de seu ciclo de vida. Uma implementação ampla e inclusiva de um **Programa de Governança em Privacidade** é necessária para gerenciar riscos, em ascensão, nas mais variadas áreas. Aumentar a confiança de todas as partes interessadas necessita que os gestores do gerenciamento de segurança e risco ampliem tanto a frequência quanto a amplitude da comunicação, para assim assegurar que o uso dos dados pessoais seja granular, com finalidades específicas e com riscos mapeados e sob controle.

As orientações relativas à elaboração do **Programa de Governança em Privacidade** foram estruturadas em dois capítulos:

- O Capítulo 1 destaca sua composição; e
- O Capítulo 2 trata sobre suas etapas e como elaborá-las.

Este documento será atualizado e ampliado permanentemente, com o objetivo de manter alinhamento com as diretrizes determinadas pela Autoridade Nacional de Dados Pessoais (ANPD). Além disso, o modelo de **Programa de Governança em Privacidade** aqui apresentado não é restritivo e o objetivo buscado não é sua rigorosa adoção. Como cada órgão e entidade possui características e especificidades próprias, o modelo deve ser adaptado para cada caso específico.

1 – PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

1.1 – O que é

A Lei 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), em sua Seção II, Das Boas Práticas e da Governança, informa, no Art. 50 § 2º sobre as características mínimas de um **Programa de Governança em Privacidade – PGP**, conforme apresentado na Figura 1:

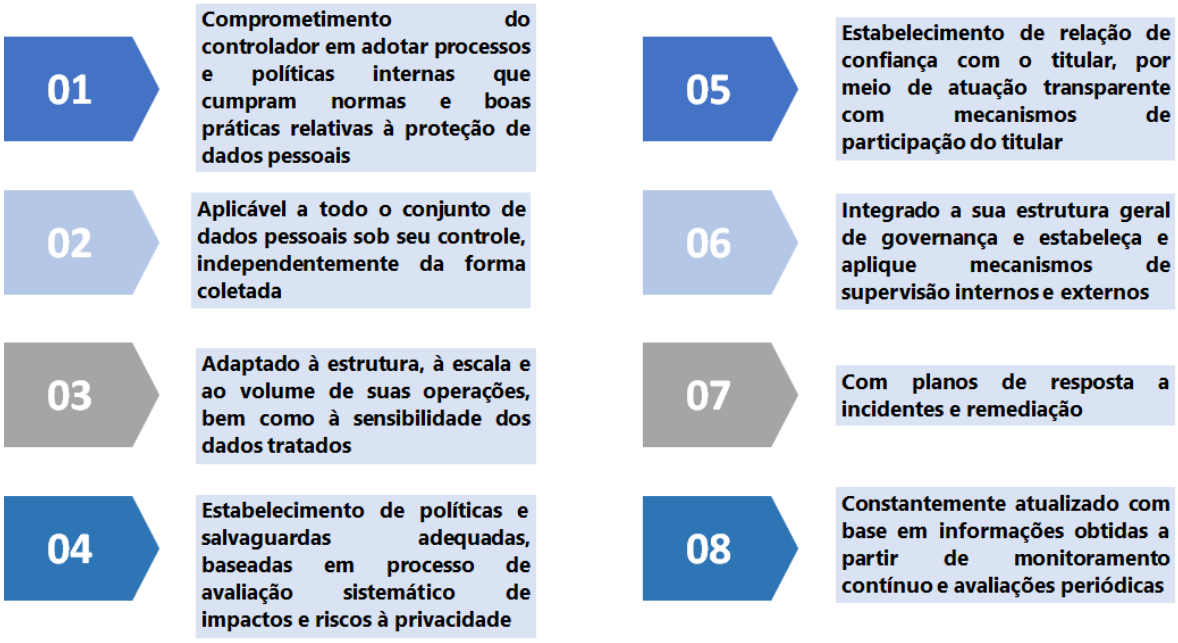

Figura 1. Características Mínimas de um Programa Gerenciamento de Privacidade - LGPD

Diante das características de um **Programa de Governança em Privacidade – PGP** apresentadas pela LGPD é necessário também destacar seus principais atores:

- No papel central, por sua importância, tem-se o **titular**, qualquer pessoa natural, protegida pelo princípio da autodeterminação informativa (inciso III do art. 2º da Lei Geral de Proteção de Dados);
- A seguir, o **controlador**, pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (inciso VI do art. 5º da Lei Geral de Proteção de Dados). O controlador pode exercer diretamente o tratamento dos dados. Mas pode, também, designar um operador;
- O **operador** é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (inciso VII do art. 5º da Lei Geral de Proteção de Dados). Ambos, controlador e

operador, recebem a nomeação de "agentes de tratamento" (inciso IX do art. 5º da Lei Geral de Proteção de Dados);

- O **encarregado** corresponde a uma pessoa natural inequivocamente investida nessa função (que, na legislação europeia, corresponde ao *Data Protection Officer* - DPO). Sua incumbência é de fazer a intermediação entre o titular e os agentes de tratamento, mas também entre estes agentes e a Autoridade Nacional de Proteção de Dados - ANPD - (inciso VII do art. 5º da Lei Geral de Proteção de Dados);
- finalmente, a **Autoridade Nacional de Proteção de Dados - ANPD** tem a missão de regular o setor de tratamento de dados pessoais. Está autorizada, portanto, a agir em proteção aos princípios e fundamentos da Lei Geral de Proteção de Dados.

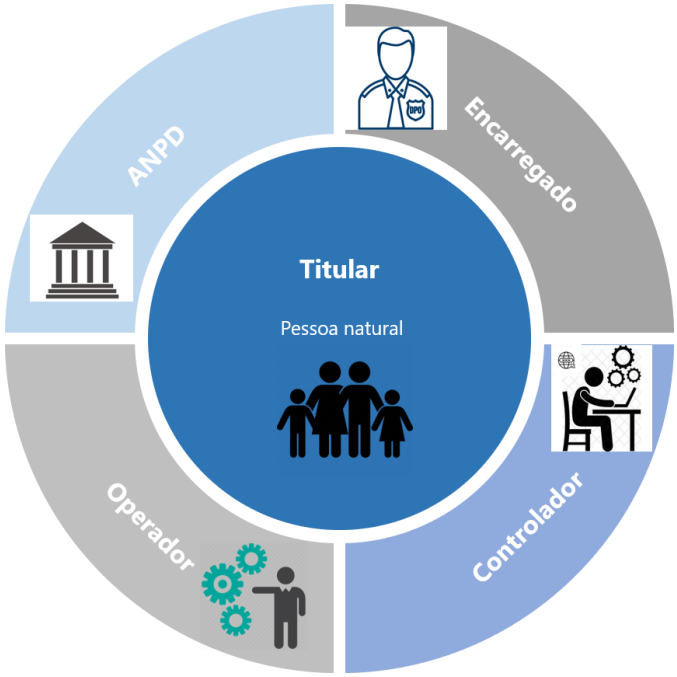

Figura 2. Atores LGPD

Vale ressaltar que, ao contrário de um projeto, que tem início, meio e fim, um programa estabelece uma metodologia abrangente que influenciará permanentemente os processos de tomada de decisão com base em riscos e melhorias contínuas na maturidade. Pode-se, entretanto, criar projetos para se alcançar objetivos do programa. Na criação de projetos para se alcançar objetivos do programa, deve-se selecionar a metodologia mais adequada a realidade institucional. Após a escolha da metodologia é necessário definir:

- os objetivos, as metas e os indicadores;

- os líderes responsáveis por cada frente de atuação do projeto (interação com o cidadão, operações de TI, segurança, jurídico, operadores, entre outros); e

- canais de comunicação com os líderes, cidadãos, com os operadores e também com a Autoridade Nacional de Proteção de Dados - ANPD.

Por fim, recomenda-se ainda criar modelos padronizados para obtenção de respostas que subsidiarão reportes para a alta administração.

1.2 – Estruturação

A estrutura do **PGP** apresentada neste documento é inspirada no ciclo PDCA (*Plan, Do, Check e Act*) bem como nas normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27701:2019. Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação e ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

O **programa** foi estruturado nas seguintes etapas, conforme Figura 3, e serão descritas e detalhadas no próximo capítulo:

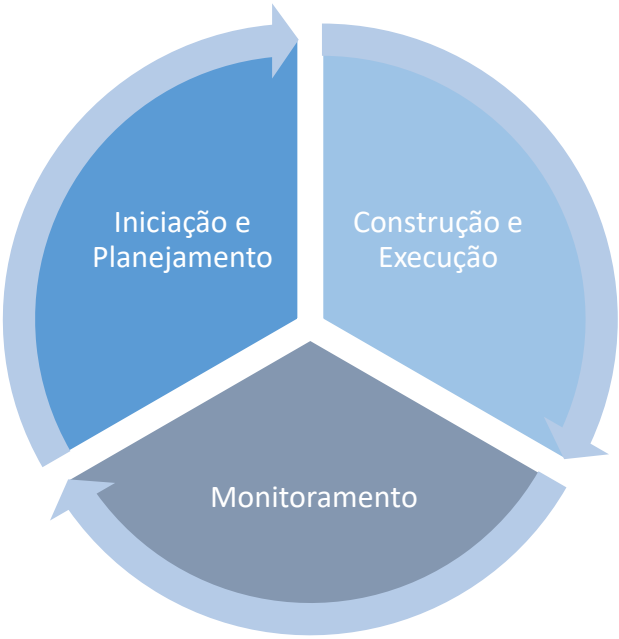

Figura 3. Etapas Programa de Governança em Privacidade – PGP

2 – ETAPAS DO PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

2.1 – Iniciação e Planejamento

A etapa de Iniciação e Planejamento busca compreender quais são as primeiras informações e os dados importantes que devem ser conhecidos. Com isso em mente, essa etapa é constituída pelos marcos apresentados na Figura 4, que serão detalhados a seguir.

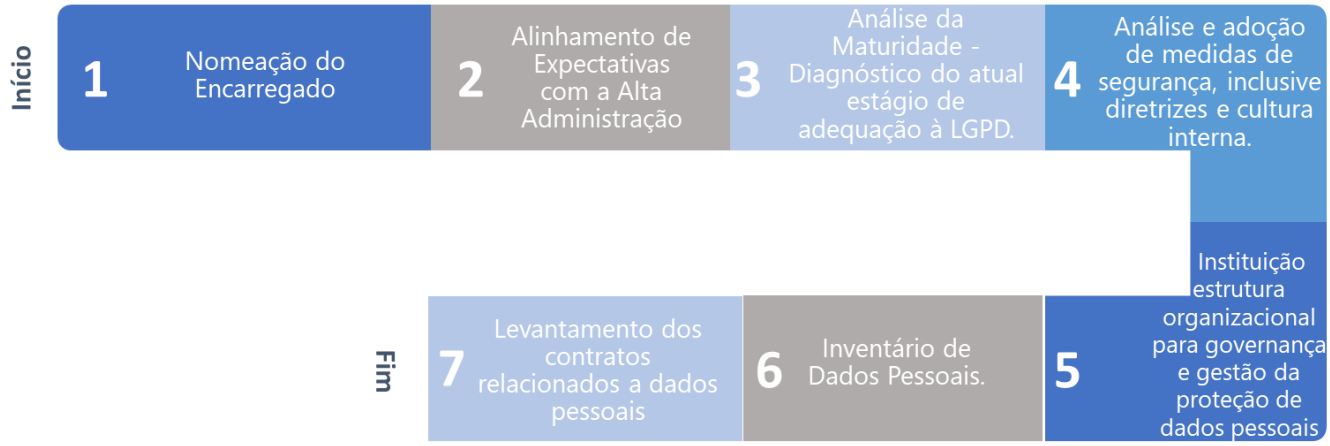

Figura 4. Marcos Etapa Iniciação e Planejamento

Recomenda-se que o início seja dado pela nomeação do Encarregado, que conduzirá a instituição, em conjunto com o Comitê de Governança Digital, segundo o Art. 2º do Decreto nº 10.332, de 28 de abril de 2020[1]. De acordo com o referido decreto, o encarregado é um dos membros do Comitê de Governança Digital do respectivo órgão, que tem como objetivo deliberar sobre os assuntos relativos à implementação das ações de governo digital e ao uso de recursos de tecnologia da informação e comunicação.

O início também deve incluir a criação de uma estrutura organizacional para compor o conhecimento de dados pessoais em toda a entidade ou órgão, além de supervisionar as três etapas de ação para criar e manter o **Programa de Governança em Privacidade.**

2.1.1 – O Encarregado

A indicação do encarregado deve acontecer no início do **PGP**. Conforme o Art. 5º inciso VIII da LGPD, o encarregado é a pessoa indicada pelo controlador e operador para

[1] Disponível em <https:// http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10332.htm>

atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD. Entre as competências de um encarregado apresentadas na LGPD, pode-se citar:

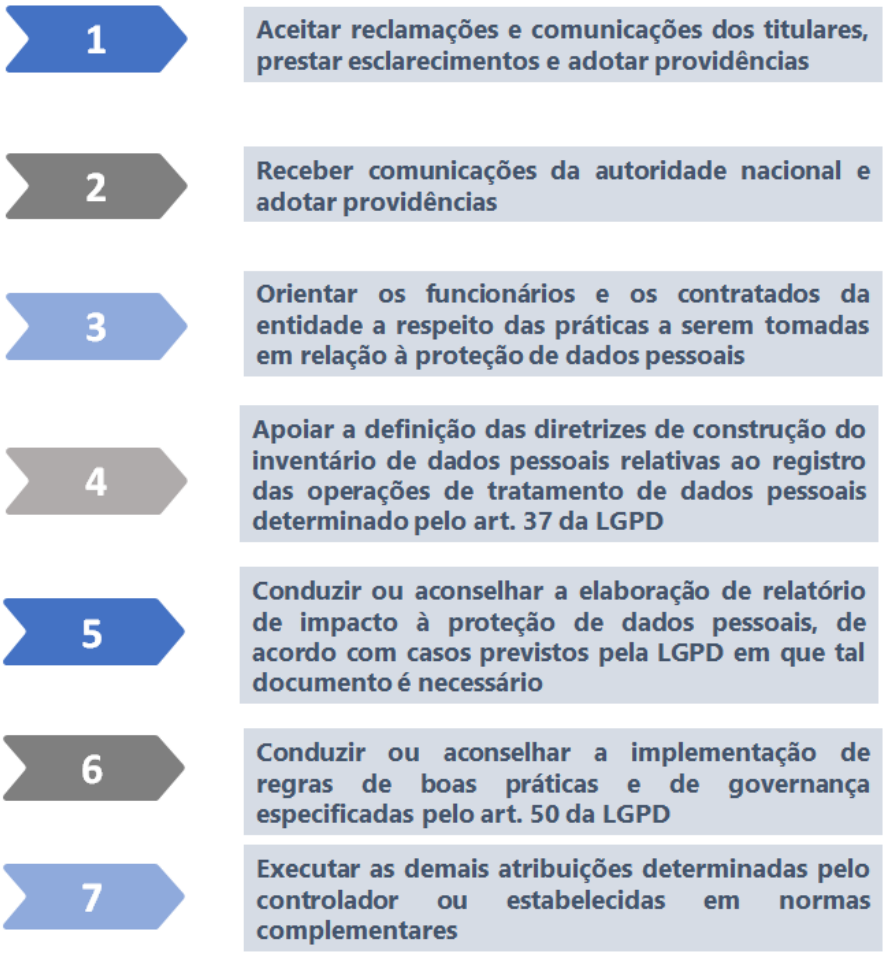

Figura 5. Competências Encarregado - LGPD[2]

Além das competências elencadas pela LGPD, é importante que sejam considerados requisitos de experiência, conhecimentos e formação para o desempenho da função de encarregado. Assim, com base em inspiração resultante de pesquisa realizada em publicações associadas à *General Data Protection Regulation* (GDPR)[3][4] recomenda-se que também sejam considerados para designação do encarregado os requisitos listados na Figura 6.

[2] Item 5 da Figura 5: conforme seção 2.5.2.2 do Guia de Boas Prática LGPD
[3] Article 29 Data Protection Working Party WP 243 revi.01 The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data
[4] The DPO Handbook Guidance seção 2.5.3

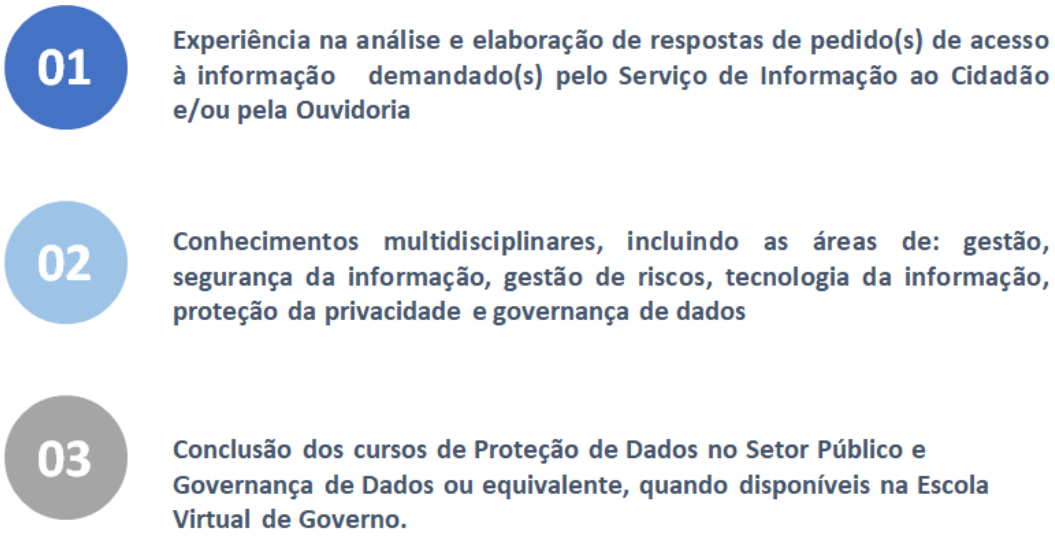

Figura 6. Requisitos Encarregado

É importante, ainda, que o encarregado tenha independência para determinar a aplicação de recursos e as ações necessárias, bem como o pronto apoio das unidades administrativas no atendimento das solicitações de informações em relação às operações de tratamento de dados pessoais. Também deve ter amplo acesso a estrutura organizacional, investigar proativamente os níveis de conformidade e instruir os responsáveis pelos riscos a corrigir as lacunas encontradas.

É válido destacar que o apoio da alta administração é essencial para o sucesso do trabalho executado pelo encarregado, incluindo seu envolvimento nas decisões e recursos suficientes para pessoal, treinamento, entre outros. Os órgãos da Administração Pública também devem assegurar ao encarregado uma estrutura organizacional suficiente para governança e gestão da proteção de dados pessoais, conforme o porte da instituição. Nessa linha, o encarregado necessita também de autonomia e independência funcional para avaliação das atividades de tratamento de dados pessoais realizadas pelo órgão e um contínuo aperfeiçoamento por meio de treinamentos e capacitações realizadas com segurança da informação e proteção de dados pessoais.

Diante da nítida importância do encarregado para a implementação da LGPD e, consequentemente, para o **PGP**, a seguir é apresentada uma proposta de tópicos a serem abordados, analisados e tratados pelo encarregado. É recomendado que o trabalho a ser executado pelo encarregado também seja dividido em etapas e os seguintes passos são sugeridos:

Encarregado - Etapa de Iniciação e Planejamento

- Alinhamento de expectativas entre o encarregado e a alta direção do órgão;
- Apresentação, para as secretarias do órgão (secretários, diretores e coordenadores), do papel exercido pelo encarregado como relevante e influenciador;
  - Como o encarregado pode servir e agregar valor ao órgão, dado o disposto na LGPD;
  - Confirmar e garantir aos servidores do órgão que, enquanto representante interno da ANPD, seu papel deve ser uma assistência de grande valor e não um obstáculo;
- Priorização e foco em melhorias, tendo consciência da estrutura, dos requisitos de dados pessoais, bem como da maturidade de *compliance* do órgão;
  - Lançamento e implementação de mecanismos para geração de relatórios internos de atividades de processamento de dados pessoais, sejam tais atividades novas, majoritárias ou com alterações;
  - Conclusão de um inventário de dados pessoais, destacado no início desta seção, com a lista dos principais serviços que utilizam dados pessoais do órgão.
- Alcance de credibilidade e valor entre os dirigentes do órgão;
- Instituição e coordenação, em conjunto com o Comitê de Governança Digital do órgão ou entidade, de uma:
  - Estrutura Organizacional para Governança e Gestão da Proteção de Dados Pessoais.
- Apresentação de minuta de política de privacidade aos dirigentes do órgão, com o comprometimento de revisar, conforme os apontamentos de melhorias sugeridos;
- Projeção ou refinamento de uma nova estratégia de privacidade: um mapeamento do atual cenário e fornecimento de uma visão geral do orçamento necessário para, no mínimo, os próximos 12 meses, bem como a associação e o relacionamento aos pontos de atenção listados;
- Neste início sugere-se concentrar em poucos assuntos, balanceando entre as áreas de maior risco e as mais simples do órgão, quanto a privacidade dos dados. Por

exemplo, alternar entre o projeto com maior risco, no que envolve dados pessoais, e uma campanha de sensibilização para os servidores.

Quadro 1: Encarregado - Etapa de Iniciação e Planejamento

2.1.2 - Alinhamento de Expectativas com a Alta Administração

Ao longo da etapa de Iniciação e Planejamento é importante ainda alinhar as expectativas com a alta administração, priorizando as ações mais urgentes, sem esquecer de mencionar os projetos e as estruturas da organização envolvidas. Considera-se como alta administração: Ministros de Estado, ocupantes de cargos de natureza especial, ocupantes de cargo de nível 6 do Grupo-Direção e Assessoramento Superiores - DAS e presidentes e diretores de autarquias, inclusive as especiais, e de fundações públicas ou autoridades de hierarquia equivalente. É importante destacar que o alinhamento com a Alta administração e a priorização de ações urgentes guiam o estabelecimento da cultura de proteção de dados na instituição.

2.1.3 – Maturidade da Organização

Outro ponto a se analisar é a maturidade da organização, observando fatores como a rastreabilidade de dados - estruturando-os e descrevendo as informações tratadas em cada sistema -, a comunicação com o cidadão e a transparência (elaborando, por exemplo, a política de privacidade e termos de uso de serviços, bem como a comunicação sobre o uso de cookies). Como ferramenta para a análise da maturidade, a Secretaria de Governo Digital (SGD), com o intuito de fornecer um diagnóstico do atual estágio de adequação à LGPD[5], trazendo subsídios para a formalização e cálculo de um índice de maturidade, oferece um questionário aos órgãos do SISP. Esse diagnóstico disponível no portal gov.br é uma versão de degustação e tem o propósito de auxiliar constantes medições do índice de maturidade do órgão ou entidade em relação à LGPD. Além de retratar o nível de adequação à LGPD, o índice de maturidade é também utilizado como um índice de performance e será apresentado na etapa de Monitoramento do **PGP**, item 2.3.1 deste Guia.

[5] Disponível em <https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnostico-de-adequacao-a-lgpd>

2.1.4 – Medidas de Segurança

Na etapa de Iniciação e Planejamento, medidas de segurança também devem ser analisadas e adotadas, revisando e propondo aprimoramento das diretrizes e cultura internas. Nesse cenário, uma das ferramentas que podem auxiliar na construção do **PGP** como um todo é o Guia de Boas Práticas da LGPD[6]. Com o objetivo de fornecer orientações de boas práticas aos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional para as operações de tratamento de dados pessoais, conforme previsto no art. 50 da LGPD, o Comitê Central de Governança de Dados (CCGD)[7] instituído pelo Decreto 10.046, de 9 de outubro de 2019, publicou o Guia para propor caminhos que levem à sustentabilidade das ações de proteção aos dados pessoais para um país que hoje se projeta como uma potência na transformação digital de governo.

2.1.5 – Estrutura Organizacional para Governança e Gestão da Proteção de Dados Pessoais

Recomenda-se ainda, como suporte para a estrutura do **PGP**, assim como para a realização das atividades do encarregado provenientes de sua atuação como canal de comunicação entre o controlador, os titulares dos dados e a ANPD o estabelecimento de uma estrutura organizacional para governança e gestão da proteção de dados pessoais, de acordo com o porte da instituição. Como referência e sugestão de estruturação, a Portaria da Anatel nº 1.197, de 25 de Agosto de 2020[8] apresenta, entre outras informações, as competências de um Escritório de Apoio a Proteção de Dados, que representa, com êxito, a estrutura recomendada.

2.1.6 – Inventário de Dados Pessoais

Para obter um mapeamento dos dados pessoais utilizados pelo órgão, recomenda-se a realização de um inventário de dados, especialmente dos dados pessoais. Conforme o

[6] Disponível em <https:// https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd>
[7] Disponível em < https://www.gov.br/governodigital/pt-br/governanca-de-dados/comite-central-de-governanca-de-dados>
[8] Disponível em < https:www.in.gov.br/en/web/dou/-/portaria-n-1.197-de-25-de-agosto-de-2020-274640686>

Guia de Elaboração de Inventário de Dados Pessoais, o Inventário de Dados Pessoais representa documento primordial no sentido de documentar o tratamento de dados pessoais realizados pela instituição, em alinhamento ao previsto pelo art. 37 da LGPD. O inventário consiste em uma excelente forma de fazer um balanço do que o órgão e entidade faz com os dados pessoais, identificando quais dados pessoais são tratados, onde estão e que operações são realizadas com eles.

No Guia de Elaboração de Inventário de Dados Pessoais, a Secretaria de Governo Digital (SGD) propõe aos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) um modelo simplificado de inventário de dados pessoais, baseado nas metodologias adotadas pela Bélgica, Inglaterra e França, visando identificar as operações de tratamento de dados pessoais realizadas pela instituição no papel de controlador (LGPD, art. 5º, VI). Estruturado em formato de planilha eletrônica, é uma abordagem top/down, onde o serviço e os processos de negócio, e não os dados propriamente ditos, são analisados. Atualizado regularmente, o inventário permitirá atender tanto o requisito de manter um registro das operações de tratamento de dados pessoais, quanto o de auxiliar no controle do atendimento aos princípios, ambos estabelecidos pela LGPD.

2.1.7 – Levantamento de Contratos relacionados a Dados Pessoais

O levantamento dos serviços que tratam dados pessoais no Inventário de Dados viabiliza a realização de uma correlação com os contratos que os suportam. Esse mapeamento dos contratos que coletam, transferem e processam dados pessoais contribui para possíveis e necessárias adequações contratuais, tanto nos contratos existentes, quanto nos futuros.

2.2 – Construção e Execução

Além do texto apresentado na LGPD, pode-se inferir da ABNT ISO/TR 18638:2019 que, considerando os órgãos da Administração Pública Federal (APF), um **PGP** deve ser projetado para proteger os direitos do cidadão em relação à privacidade da informação e deve ser desenvolvido e implementado seguindo as leis jurisdicionais relevantes.

Assim, na etapa de construção de um programa de gerenciamento da privacidade, deve-se considerar os pontos de atenção listados na Figura 7.

Figura 7. Considerações Etapa de Construção e Execução

Logo, neste capítulo, os marcos a serem alcançados na etapa de Construção e Execução, apresentados na Figura 8, serão descritos e detalhados.

Figura 8. Marcos Etapa Construção e Execução

2.2.1 – Políticas e práticas para proteção da privacidade do cidadão

Na construção de um **PGP** devem ser especificadas políticas e práticas para proteger a privacidade do cidadão, garantindo que todos os usos dos dados pessoais são conhecidos

e adequados de acordo com as leis, bem como sua proteção contra mau uso ou revelação inadvertida ou deliberada. Além das políticas e práticas, na Administração Pública, papéis específicos dos servidores envolvidos na coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais devem ser colocados em prática, assim como a educação dos colaboradores em relação a políticas e práticas de proteção de privacidade e dos cidadãos em relação aos seus direitos quanto à privacidade da informação.

Informações como a finalidade do órgão ou entidade e a base legal para tratamento de dados, obtidas no inventário dos dados pessoais, realizado na fase de Iniciação e Planejamento, são úteis na construção das operações de tratamento. Tais informações auxiliam na determinação dos detalhes do ciclo de vida dos dados pessoais, por exemplo a finalidade do tratamento, como, onde e por quanto tempo é o armazenamento, entre outros.

2.2.2 – Cultura de segurança e proteção de dados e Privacidade desde a Concepção (privacy by design)

A promoção de uma cultura de segurança e proteção de dados deve ser tratada na etapa de construção e execução de um **PGP** com o intuito de comunicar os objetivos, metas e indicadores utilizados, além de divulgar o papel da Administração Pública como custodiante dos dados e sua responsabilidade ao tratar os dados pessoais dos cidadãos. As informações do **PGP** devem ser disponibilizadas de forma clara e eficiente, além de estarem facilmente acessíveis. Capacitação e treinamento devem ser oferecidos para que uma cultura de Privacidade desde a Concepção (*privacy by design*) seja instituída.

O conceito de Privacidade desde a Concepção significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo. Conforme o Guia de Boas Práticas da LGPD, tal privacidade pode ser alcançada por meio da aplicação dos 7 Princípios Fundamentais (Cavoukian, 2009), listados a seguir:

- Proativo, e não reativo; preventivo, e não corretivo: A abordagem de Privacidade desde a Concepção (PdC) antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. Desse modo, não espera que riscos de privacidade se materializem, nem oferece soluções para as infrações de privacidade após a ocorrência, mas visa impedir que eles ocorram.
- Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio: Busca-se oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam

protegidos automaticamente em qualquer sistema de TI ou prática de negócios. É uma forma de evitar que qualquer ação seja necessária por parte do titular dos dados pessoais para proteger a sua privacidade, pois ela já estará embutida no sistema, por padrão.

- Privacidade incorporada ao projeto (*design*): A privacidade deve estar incorporada ao projeto e arquitetura dos sistemas de TI e práticas de negócios, não deve ser considerada como complemento adicional, após o sistema, projeto ou serviço já estar em implementação ou em execução. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade.
- Funcionalidade total: A PdC não envolve simplesmente a formalização de declarações e compromissos de privacidade. Refere-se a satisfazer todos os objetivos do projeto, não apenas os objetivos de privacidade, permitindo funcionalidade total com resultados reais e práticos. Ao incorporar privacidade em uma determinada tecnologia, processo ou sistema, isso é realizado de uma forma que não comprometa a plena funcionalidade e permita que todas as exigências do projeto sejam atendidas.
- Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados: Por ser incorporado ao sistema antes de o primeiro elemento de informação ser coletado, a PdC estende-se por todo o ciclo de tratamento dos dados envolvidos no projeto, sistema ou serviço. Medidas fortes de segurança são essenciais para a privacidade, do início ao fim.
- Visibilidade e Transparência: A PdC objetiva garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, está de fato operando de acordo com as premissas e objetivos declarados, os quais devem ser objeto de verificação independente. Visibilidade e transparência são essenciais para estabelecer responsabilidade e confiança.
- Respeito pela privacidade do usuário: Acima de tudo, a privacidade desde a concepção exige que as instituições respeitem os direitos dos titulares dos dados pessoais. Isso é alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular dos dados. Os melhores resultados da privacidade desde a concepção, geralmente, são aqueles projetados de acordo com os interesses e necessidades dos titulares dos dados pessoais, que têm o maior interesse em gerenciar seus próprios dados.

2.2.3 – Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

É ainda na etapa de Construção e Execução do **PGP** que o Relatório de Impacto à Proteção de Dados Pessoais - RIPD deve ser elaborado. O RIPD representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição e serve tanto para a análise quanto para a documentação do tratamento dos dados pessoais. O RIPD visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

O Guia de Boas Práticas da LGPD, em sua seção 2.5 apresenta orientações no sentido de auxiliar os órgãos e entidades a elaborar um RIPD.

2.2.4 – Medidas e Política de Segurança da Informação e Política de Privacidade

Ainda na etapa de Construção e Execução do **PGP**, tem-se o desenvolvimento e/ou a atualização das diretrizes internas de proteção de dados pessoais. Deve ser verificado se não há tratamento excessivo de dados, se os controles de segurança são suficientes para os dados tratados, se é necessário a retenção de determinados dados tratados e se é necessário revisar contratos. Desse modo, torna-se fundamental o desenvolvimento de uma política de segurança da instituição, conforme a Instrução Normativa n. 1 de 27 de maio de 2020[9], do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), bem como de uma política de privacidade de dados.

Também é necessário a elaboração de uma Política de Privacidade. Conforme o Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos[10] a Política de Privacidade é um documento informativo pelo qual o prestador de serviço transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário. A Política de Privacidade, que faz parte do Termo de Uso, origina-se da responsabilidade de os agentes de tratamento de dados serem transparentes com o titular de dados e informarem como as atividades de tratamento de dados atendem os

[9] Disponível em <https:// https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215>
[10] Disponível em < https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaTermoUso.pdf>

princípios dispostos no artigo 6º LGPD. Portanto, o documento é, ao mesmo tempo, um dever do controlador e um direito do titular. Assim, de acordo com o Guia de elaboração de Termo de Uso e Política de Privacidade, o serviço deve informar ao titular do dado como ele fornece a privacidade necessária para que a confidencialidade dos dados prestados pelos titulares dos dados seja garantida de forma eficiente e como os princípios abaixo são atendidos.

- Finalidade: Obrigatoriedade de tratamento somente para fins legítimos, específicos, explícitos, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (art. 6º, I);
- Adequação: Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento (art. 6º, II);
- Necessidade: Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (art. 6º, III);
- Livre acesso: Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (art. 6º, IV).
- Qualidade dos dados: Critérios de qualidade dos dados, para garantir, aos titulares, a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (art. 6º, V).
- Transparência: Critérios de transparência, para garantir, aos titulares, o fornecimento de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (art. 6º, VI).
- Segurança: Critérios de segurança, para que se utilize medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (art. 6º, VII);
- Prevenção: Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6º, VIII);
- Não discriminação: Critérios de não discriminação, para garantir que não se realize o tratamento de dados para fins discriminatórios ilícitos ou abusivos (art. 6º, IX).

- Responsabilização e prestação de contas: para que, para cada tratamento de dados se possa demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (art. 6º, X).

Sugere-se que uma Política de Privacidade contenha os tópicos apresentados no Quadro 2:

1 – Controlador
2 – Operador
3 – Encarregado
4 - Quais dados são tratados
5 – Como os dados são coletados
6 – Qual o tratamento realizado e para qual finalidade
7 – Compartilhamento de dados
8 – Segurança dos dados
9 – Cookies
10 – Tratamento posterior dos dados para outras finalidades
11 – Transferência internacional de dados

Quadro 2 Tópicos Política de Privacidade

As medidas de segurança para a proteção dos dados pessoais devem ser implementadas na fase de Construção do Programa de Governança em Privacidade. Segurança desde a Concepção (*security by design*) e a importância de se tomar medidas preventivas precisam ser consideradas, bem como a gestão dos riscos, a gestão de incidentes e a violação dos dados.

Por fim, mas não menos importante, os direitos dos titulares precisam ser gerenciados. Devem ser destacadas e elucidadas questões como a diferença entre o titular e o custodiante do dado pessoal, do ponto de vista da Administração Pública, bem como as obrigações quanto ao fornecimento de informações aos titulares com relação ao tratamento dos dados pessoais, termo de uso e política de privacidade.

2.2.5 – Adequação Cláusulas Contratuais

Para adaptar os contratos, convênios e outros instrumentos que impliquem no tratamento de dados pessoais, mapeados pelo Inventário realizado na etapa de Iniciação e Planejamento, é importante rever os documentos vigentes e os dados já coletados. No âmbito dos contratos administrativos, pode ser necessário que a Administração Pública revisite as cláusulas contratuais econômicas firmadas, mesmo após concluído o certame. Pode ser preciso incluir novas cláusulas, conforme os princípios da LGPD, apresentados em seu art. 6º. Como um dos princípios listados é a transparência, torna-se essencial que o contrato apresente informações claras e objetivas, abordando, se pertinente:

- Delimitações claras e objetivas das responsabilidades do controlador e operador;
- A forma que é realizada a coleta e o tratamento de dados;
- A existência da possibilidade de o titular acessar os seus dados coletados;
- A forma que é realizada a correção, bloqueio ou eliminação de dados mediante solicitação do titular;
- A existência da possibilidade de revogação do consentimento dado pelo titular;
- O detalhamento de quem tem acesso aos dados, o responsável por seu uso e tratamento, a forma de armazenamento e as particularidades de possíveis auditorias;
- As medidas de proteção e segurança dos dados coletados e armazenados pela contratada.

2.2.6 – Termo de Uso

Conforme o Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos, publicado pela SGD, Termo de Uso é um documento que fornece uma descrição detalhada do serviço, das condições e das regras aplicáveis a ele.

O Termo de Uso, como a Política de Privacidade, advém da consciência do controlador e operador ser transparente com o titular de dados pessoais e comunicar como as atividades de tratamento desses dados observam os princípios dispostos no artigo 6º da LGPD. Em cumprimento aos princípios da publicidade e da transparência, e a fim de assegurar aos cidadãos amplo acesso às informações, os termos devem ser regularmente

atualizados a fim de refletir, de modo claro e preciso, as finalidades de coleta, uso, armazenamento, tratamento e proteção dos dados pessoais dos titulares, que comumente serão utilizados pelo órgão e entidade no exercício de suas competências legais ou execução de políticas públicas, devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

Os tópicos que devem constar no Termo de Uso estão listados no quadro a seguir:

1. Aceitação dos Termos e Políticas
2. Definições
3. Arcabouço Legal
4. Descrição do serviço
5. Direitos do usuário
6. Responsabilidades do usuário e da Administração Pública
7. Mudanças no Termo de Uso
8. Informações para contato
9. Foro

Quadro 3 Tópicos Termo de Uso

2.2.7 – O Encarregado

Recomenda-se que o encarregado, na etapa de Construção/Execução, realize as atividades apresentadas no quadro a seguir.

Encarregado - Etapa de Construção e Execução
- Implementação das ações identificadas na fase de Iniciação e Planejamento; - Demonstração, para os dirigentes do órgão, do progresso e dos resultados obtidos com as atividades envolvendo o inventário dos dados e a divulgação e conscientização da LGPD junto aos servidores.

- Se necessário, redefinição de prioridades, baseando-se nos resultados alcançados e no retorno dos dirigentes e secretarias do órgão. - Estabelecimento e manutenção de documentação relacionada à LGPD e aos dados pessoais tratados no órgão, com informações sobre: atividades em andamento e planejadas; responsáveis pelos serviços e sistemas que utilizam dados pessoais; e incidentes e vazamento de dados pessoais. - Definição de mecanismos de reportes internos, assegurando transparência e rapidez na troca de informação, além de reafirmar o papel como facilitador, suporte e nunca um obstáculo.

Quadro 4: Encarregado - Etapa de Construção e Execução

2.3 – Monitoramento

Acompanhar a conformidade à LGPD é uma atividade contínua e necessária para os órgãos e entidades manterem **PGP** a longo prazo. Assim sendo, esta última etapa do **PGP** aborda aspectos, detalhados nas próximas seções, que incluem, em grande parte, coleta e análise de informações, bem como elaboração de relatórios e apresentações de resultados. A Figura 9 apresenta os marcos da Etapa de Monitoramento, que serão apresentados a seguir.

Figura 9. Marcos Etapa Monitoramento

2.3.1 – Indicadores de Performance

Os Indicadores de Performance (*Key Performance Indicator* - KPI) incluem a análise regular dos principais indicadores de desempenho para verificar lacunas no Programa de Governança em Privacidade assim como o status de outras iniciativas de privacidade. Recomenda-se o uso dos seguintes indicadores:

- Monitoramento e acompanhamento do número de incidentes de violação de dados pessoais e/ou vazamento de dados pessoais;
- Resultados do Diagnóstico de Adequação à LGPD - índice de adequação;
- Índice de serviços com dados pessoais inventariados: número de serviços com dados pessoais inventariados / número de serviços com dados pessoais do órgão * 100;
- Índice de serviços com termo de uso elaborado: quantidade de serviços com termo de uso elaborado / quantidade de serviços do órgão * 100;
- Índice de serviços com RIPD elaborado: quantidade de serviços com RIPD elaborado / quantidade de serviços do órgão * 100;
- Índice de conscientização em segurança: quantidade de treinamentos realizados / quantidade de treinamentos previstos * 100;
- Índice de quantidade de controles de segurança e privacidade implementados para um determinado serviço: quantidade de controles de segurança e privacidade implementados para um determinado serviço / quantidade total de controles de segurança e privacidade identificados para o serviço * 100.

2.3.2 – Gestão de Incidentes

É importante incluir nesta etapa do **PGP** um processo de Gestão de Incidentes, que registre os incidentes de segurança da informação e de privacidade ocorridos e que armazene informações como: a descrição dos incidentes ou eventos; as informações e sistemas envolvidos; as medidas técnicas e de segurança utilizadas para a proteção das informações; os riscos relacionados ao incidente e as medidas tomadas para mitigá-los a fim de evitar reincidências.

É válido também implementar e manter controles e procedimentos específicos para detecção, tratamento, coleta/preservação de evidências e resposta a incidentes de segurança da informação e privacidade, de forma a reduzir o nível de risco ao qual a Solução de TIC e/ou o órgão estão expostos, considerando os critérios de aceitabilidade de riscos definidos pelo órgão.

É recomendado ainda que a Gestão de Incidentes possua um Plano de Comunicação orientando a forma que os incidentes de segurança, que acarretem risco ou dano, sejam informados aos órgãos fiscalizatórios e à imprensa.

2.3.3 – Análise e Reporte de Resultados

A análise e o reporte de resultados também é indicado na etapa de monitoramento para demonstrar o valor do **PGP** para a alta administração. Mostrar a evolução das ações e resultados obtidos, bem como o papel da privacidade para o cidadão reforçam e fortalecem a cultura de privacidade dos dados.

2.3.4 – O Encarregado

O encarregado, dado seu papel de articulação, exerce função fundamental nessa etapa, conforme apontado no quadro a seguir.

Encarregado - Etapa de Monitoramento
- Gerenciamento do estabelecimento de métricas para auxiliar no acompanhamento das ações do Programa de Governança em Privacidade; - Divulgação dos resultados entre as diversas áreas do órgão - estabelecimento de uma estrutura de divulgação de resultados para a alta direção dos órgãos e entidades.

Quadro 5: Encarregado - Etapa de Monitoramento

A incorporação, em um **PGP,** de todos os passos apresentados nas 3 etapas, listados na Figura 10, ajudará a garantir que o programa abordará os regulamentos de privacidade

de dados e ajudará a criar e conquistar a confiança do cidadão titular dos dados por meio da demonstração do cuidado com seus dados pessoais e sua privacidade.

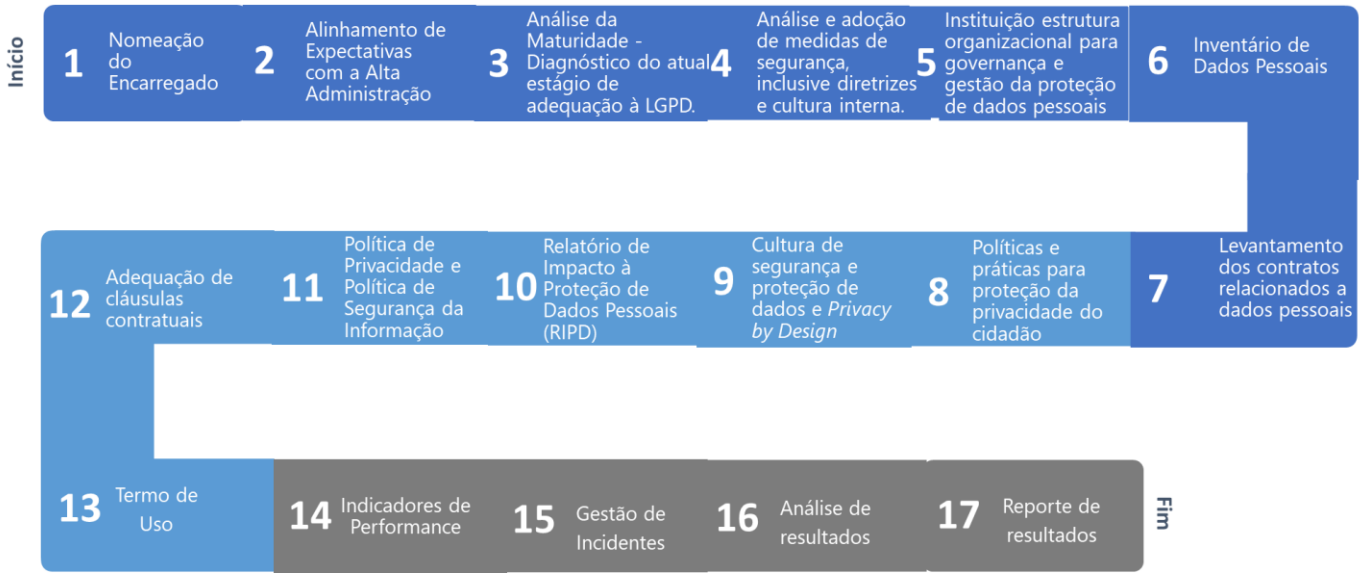

Figura 10. Passos das Etapas do Programa de Governança em Privacidade

Referências Bibliográficas

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2013. Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação.

_____. ABNT NBR ISO/IEC 27001:2013. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.

_____. ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

_____. ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT ISO/TR 18638:2019- Informática em saúde — Orientações sobre educação da privacidade das informações em saúde em organizações de assistência à saúde.

ARTICLE 29 DATA PROTECTION WORKING PARTY. WP29 guidelines on the Data Protection Officer requirement in the GDPR. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025. Acesso em: 19 ago. 2020.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 20 ago. 2020.

Cavoukian, Ann. Privacy by Design: The 7 Foundational Principles. August, 2009. Disponível em: https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf. Acesso em: 13 jan. 2020.

IBM RATIONAL UNIFIED PROCESS. Um processo proprietário de Engenharia de software. IBM, 2003.

GARTNER GROUP. The Privacy Officer's First 100 Days. 2018. Disponível em: https://www.gartner.com/en. Acesso em: 21 ago. 2020.

KORFF, Douwe; GEORGES, Marie. The DPO Handbook: Guidance for data protection officers in the public and quase-public sectors on how to ensure compliance with the european union

general data protection regulation. Guidance for data protection officers in the public and quasi-public sectors on how to ensure compliance with the European Union General Data Protection Regulation. 2019. Disponível em: https://ssrn.com/abstract=3428957. Acesso em: 20 ago. 2020.

PROJECT MANAGEMENT INSTITUTE. Um Guia de Conhecimento em Gerenciamento de Projetos. Guia PMBOK 5a edição. Project Management Institute, 2013.